UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/791,322	03/02/2004	Dmitry Andreev	END920030143	1826

7590 01/21/2009

Andrew M. Calderon
Greenblum and Bernstein P.L.C.
1950 Roland Clarke Place
Reston, VA 20191

EXAMINER	
TABOR, AMARE F	

ART UNIT	PAPER NUMBER
2439	

MAIL DATE	DELIVERY MODE
01/21/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/791,322
Filing Date: March 02, 2004
Appellant(s): ANDREEV ET AL.

Andrew M. Calderon
Reg. No. 38,093
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed on 12/09/2008 appealing from the Final Office action mailed 07/22/2008.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

7,024,690	Young et al.	4-2006
5,497,421	Kaufman et al.	3-1996
6,539,482	Blanco et al.	3-2003
7,100,054	Wenisch et al.	8-2006

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 3-5, 8-10, 13, 14 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Young et al. (US 7,024,690 B1 - "Young") in view of Kaufman et al. (US 5,497,421 - "Kaufman"), and further in view of Blanco et al. (US 6,539,482 B1 - "Blanco")

As per Claim 1, Young teaches,

A method for authentication in a network, the method comprising: creating a credential string on a portal server [see **Client System 220** in FIG.2; and for example, col.4, lines 47-67], the credential string being an encrypted hash of a session ID [see FIG.3; and for example, col.5, lines 9-19]; and sending a UserID associated with the session ID and the credential string to a software application from the portal server [see **AP 210** in FIG.2 and FIG.3; and for example, col.5, lines 1-8].

Young teaches communicating hashed representation of user identifiers and passwords [see FIG.3 and abstract]; but fails to disclose maintaining the user password on the portal server and avoiding exposing the user password to network resources beyond the portal server. However, in the same field of endeavor, Kaufman discloses maintaining the user password on the portal server and avoiding exposing the user password to network resources beyond the portal server [see for example, FIGS.3-5 and abstract].

Therefore, it would have been obvious to a person having ordinary skill in the art, at the time of Applicants' invention, to combine the teachings of Young and Kaufman because both are in the fields of network authentication system. Incorporating Kaufman's teaching modifies the system of Young in order to protect the confidentiality of user's password [see abstract of **Kaufman**].

Young-Kaufman combination teaches confirmation request including the credential string [see for example, FIG.3 of **Young** and FIGS.3-5 of **Kaufman**]; but fails to disclose receiving a confirmation request from the software application to an LDAP; and sending a response from the LDAP proxy in reply to the confirmation request to validate the credential string to authenticate the UserID. Nevertheless, Blanco teaches receiving a confirmation request from the software application to an LDAP; and sending a response from the LDAP proxy in reply to the confirmation request to validate the credential string to authenticate the UserID [see for example, FIG.2 and abstract].

It would have been obvious to a person having ordinary skill in the art, at the time of Applicants' invention, to modify Young-Kaufman combination by incorporating Blanco's LDAP, so that users could access network service, which includes a directory, remotely or locally [see abstract of **Blanco**].

As per Claim 9, Young teaches,

A method for authenticating a user request for a software application, the method comprising: receiving a UserID and a credential string at an authentication proxy server, the credential string being an encrypted hash of a session ID, which is created at a portal [see **Client System 220** in FIG.2; and for

example, col.4, lines 47-67]; and sending a confirmation request from the authentication proxy to the a portal [see **AP 210** in FIG.2 and FIG.3; and for example, col.5, lines 1-8].

Young teaches communicating hashed representation of user identifiers and passwords [see for example, FIG.3 and abstract]; but fails to disclose maintaining the user password on the portal server and avoiding exposing the user password to network resources beyond the portal server. However, in the same field of endeavor, Kaufman discloses maintaining the user password on the portal server and avoiding exposing the user password to network resources beyond the portal server [see for example, FIGS.3-5 and abstract].

It would have been obvious to a person having ordinary skill in the art, at the time of Applicants' invention, to modify the system of Young by incorporating Kaufman's teaching in order to protect the confidentiality of user's password [see abstract of **Kaufman**].

Young-Kaufman combination teaches confirmation request including the credential string [see for example, FIG.3 of **Young** and FIGS.3-5 of **Kaufman**]; but fails to disclose receiving a confirmation request from the software application to an LDAP; and sending a response from the LDAP proxy in reply to the confirmation request to validate the credential string to authenticate the UserID. Nevertheless, Blanco teaches receiving a confirmation request from the software application to an LDAP; and sending a response from the LDAP proxy in reply to the confirmation request to validate the credential string to authenticate the UserID [see for example, FIG.2 and abstract].

It would have been obvious to a person having ordinary skill in the art, at the time of Applicants' invention, to modify Young-Kaufman combination by incorporating Blanco's LDAP, so that users could remotely or locally access network services [see abstract of **Blanco**].

As per Claim 22, Young-Kaufman-Blanco combination teaches,

A computer program product comprising a computer usable medium having readable program code embodied in the medium, the computer program product including at least one program code to:

create a credential string on a portal server, the credential string being an encrypted hash of a session ID [see **Client System 220** in FIG.2; and for example, col.4, lines 47-67 of **Young**];

send a UserID associated with the session ID and the credential string to a software application from the portal server [see **AP 210** in FIG.2 and FIG.3; and for example, col.5, lines 1-8 of **Young**], while maintaining the user password on the portal server and avoiding exposing the user password to network resources beyond the portal server [see for example, FIGS.3-5 and abstract of **Kaufman**]:

the confirmation request including the credential string [see for example, FIG.3 of **Young** and FIGS.3-5 of **Kaufman**]; receive a confirmation request from the software application to an LDAP proxy while maintaining the user password on the portal server such that the user password is not required to authenticate the User ID; and send a response from the LDAP proxy in reply to the confirmation request to validate the credential string to authenticate the UserID [see for example, FIG.2 and abstract of **Blanco**].

As per Claim 3, Young-Kaufman-Blanco combination teaches,

wherein the encrypted hash of the session ID is a derivate of the session ID [see for example, FIG.3 of **Young** and abstract of **Kaufman**].

As per Claim 4, Young-Kaufman-Blanco combination teaches,

performing a lightweight directory access protocol (LDAP) lookup using the UserID; and if the LDAP lookup confirms the UserID and the response validates the credential string [see for example, FIG.2 of **Blanco**], returning a successful authentication reply to the software application for establishing a session associated with the session ID [see for example, **Grant Access 112** in FIG.3 of **Blanco**, otherwise sending an unsuccessful authentication reply to the software application [see for example, **Deny Access 106** in FIG.3 of **Blanco**].

As per Claim 5, Young-Kaufman-Blanco combination teaches,

wherein the sending of a UserID and the credential string avoids at least one of sending a user's password outside of a portal server and storing the password in persistent memory [see for example, FIGS.3-5 and abstract of **Kaufman**].

As per Claim 8, Young-Kaufman-Blanco combination teaches,

wherein the receiving step and sending a response step is performed by an authentication proxy [see for example, **AP 210** of **Young**; **LOGIN AGENT (LA) NODE 26** of **Kaufman**; and **LDAP Client** of **Blanco**].

As per Claim 10, Young-Kaufman-Blanco combination teaches,

providing a confirmation to the software application if the response is affirmative and the UserID is authenticated by the LDAP lookup [see for example, FIGS.2 and 3 of **Blanco**].

As per Claim 13, Young-Kaufman-Blanco combination teaches,

validating the confirmation request by assuring that the credential string has been received only once for confirmation at the portal, otherwise, if presented more than once, performing at least one of initiating a security breach procedure and notifying a software application proxy [see for example, FIGS.2 and 3 – *where **Blanco** discloses credential single receiving*].

As per Claim 14, Young-Kaufman-Blanco combination teaches,

receiving the UserID and the user password during a logon to the portal, wherein the UserID is validated in the validating step and the user password is maintained at the portal and used to process the confirmation request [see for example, FIGS.3-5 and abstract of **Kaufman**].

Claims 6, 7, 15, 19 and 23-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over "Young" in view of "Kaufman", and further in view of Wenisch et al. (US 7,100,054 B2 - "Wenisch")

As per Claim 15, Young teaches,

A system for authenticating a session stored on a computer readable storage medium, comprising computer readable program code, comprising: an authentication proxy which receives requests to authenticate a UserID and a credential string [see **LOGIN AGENT (LA) NODE** in FIG.2 of **Kaufman**], the credential string being an encrypted hash of a session ID and created on a portal [see **Client System 220** in FIG.2; and for example, col.4, lines 47-67 of **Young**].

Young teaches a credential string validation component which receives requests to validate the credential string [see FIG.3]; but fails to disclose maintaining a user password on the portal such that the user password is not required to validate the credential string, and avoiding exposing the user password to network resources beyond the portal. However, Kaufman teaches maintaining a user password on the portal such that the user password is not required to validate the credential string, and avoiding exposing the user password to network resources beyond the portal [see FIGS.3-5 and abstract of **Kaufman**].

It would have been obvious to a person having ordinary skill in the art, at the time of Applicants' invention, to modify the system of Young by incorporating Kaufman's teaching in order to protect the confidentiality of user's password [see abstract of **Kaufman**].

Young-Kaufman combination fails to teach wherein the credential string validation component checks whether the credential string has been previously received for validation within a predetermined time period; however, in the same field of endeavor, Wenisch teaches wherein the credential string validation component checks whether the credential string has been previously received for validation within a predetermined time period [see for example, FIG.2; and for example, col.4, lines 25-35].

Therefore, it would have been obvious to a person having ordinary skill in the art, at the time of Applicants' invention, to modify Young-Kaufman combination by incorporating the teachings of Wenisch in order to protect the network from repetitive attack.

As per Claims 6 and 7, Young-Kaufman-Wenisch combination teaches,

sending the UserID associated with the session ID and the credential string to a software application proxy [see FIGS.3 and 3-5 of **Young** and **Kaufman** respectively. See also FIG.2 of **Blanco**]; checking whether the session ID and the credential string have been previously received within a predetermined time period; and if affirmative, initiating a security breach procedure; and wherein the security breach procedure causes the termination of any session associated with the UserID [see FIG.2; and for example, col.4, lines 25-35 of **Wenisch**].

As per Claims 19 and 23, Young-Kaufman-Wenisch combination teaches,

a software application proxy which receives the UserID and the credential string and detects whether the UserID and the credential string have been previously received within a predetermined time period; and wherein the UserID and the credential string are sent to a software application when the predetermined time period has elapsed [see FIG.2; and for example, col.4, lines 25-35 of **Wenisch**].

As per Claims 24 and 25, Young-Kaufman-Wenisch combination teaches,

wherein a network security breach is initiated when a second request to validate the credential string occurs within the predetermined time period of a first request to validate the credential string [see FIG.2; and for example, col.4, lines 25-35 of **Wenisch**]; and wherein the portal is configured to accept a logon by a user and create the credential string from an associated session ID [see for example, FIG.3 of **Young** and abstract of **Kaufman**].

Claims 16-18 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over "Young-Kaufman-Wenisch" combination, and further in view of "Blanco"

As per Claims 16-18, Young-Kaufman-Wenisch combination teaches,

wherein the authentication proxy receives the UserID and credential string from a software application [see FIGS.3 and 3-5 of **Young** and **Kaufman** respectively].

Blanco discloses wherein the authentication proxy performs lightweight directory access protocol (LDAP) lookups using the UserID and sends the credential string to the credential string validation component and receives a validation reply [see for example, FIG.2]; wherein the authentication proxy sends an affirmative authentication reply to a software application when both the LDAP lookup is successful and the validation reply indicates a valid credential string [see for example, FIG.3].

As per Claim 21, Young-Kaufman-Wenisch-Blanco combination teaches,

a lightweight directory access protocol (LDAP) directory for authenticating the UserIDs and which is accessible by the authentication proxy [see for example, FIGS.2 and 3 of **Blanco**]; and a software application proxy for intercepting the UserID and the credential string sent by the portal for monitoring duplicate occurrences of the UserID and the credential string [see FIGS.3 and 3-5 of **Young** and **Kaufman** respectively. See also FIG.2 of **Blanco**].

(10) Response to Argument

Argument (A):

Appellant argues that the rejection of Claims 1, 3-5, 8-10, 13, 14 and 22 under 35 U.S.C. 103(a) as being unpatentable over Young (US 7,024,690) in view of Kaufman (US 5,497,421), and further in view of Blanco (US 6,539,482) is in error, the decision of the Examiner to reject this claim should be reversed, and the application should be remanded to the Examiner.

Examiner respectfully disagrees.

Claims 1, 9 and 22

Appellant argues that, Kaufman does not maintain the user password on the portal and avoid exposing the user password to network resources beyond the portal.

Examiner would point out that, Kaufman's password is not maintained on the portal because when a user logs into a workstation, the login protocol computes two hash totals of the password [FIGS.3-

5 and col.4, lines 27-36]. Kaufman also discloses, "In another aspect of the invention, a login protocol enables remote authentication of the user password without transmitting the password over the network" [abstract, lines 10-13]. In addition, Kaufman discloses protecting confidentiality of user's password during remote login authentication without transmitting the password over the network [col.3, line 66 to col.4, line 14].

Appellant argues that, a private RSA key is not a password.

Examiner would point out that, the private RSA key of Kaufman was not equated with a user password in any of the previous rejections.

Appellant further argues that, Blanco does not maintain the user password on the portal and avoid exposing the user password to network resources beyond the portal.

Examiner would point out that, Blanco is applied to address other claimed features of the invention [such as: receiving a confirmation request… and sending a response…] Thus, as explained above Kaufman, not Blanco, is the reference that is applied to reject the feature 'maintain the user password on the portal and avoid exposing the user password to network resources beyond the portal' [see response to the first argument].

Claim 3

Appellant argues that, the cited portions of neither Young nor Kaufman disclose encrypted hash of the session ID being derivative of the session ID.

Examiner would point out that, FIG.3 of Young discloses calculating DIGEST [col.5, lines 61-67] of (U=user identifier, P=Password, X=random number) [steps 31 and 318] or (U, P, Y=second random number) [steps 322 and 326] and encrypted DIGEST [steps 320 and 328].

Claim 4

Appellant argues that, the cited portion of Blanco has not been shown to specifically disclose or suggest performing a lightweight directory access protocol (LDAP) lookup using the UserID and if the LDAP lookup confirms the UserID and the response validates the credential string, returning a successful authentication reply to the software application for establishing a session associated with the session ID, otherwise sending an unsuccessful authentication reply to the software application.

Examiner would point out that, FIG.2 of Blanco discloses a RADIUS authentication transaction, where the RADIUS server compares the user identifier and password such that the front end LDAP client [LDAP 22] fetch the credential data from the main directory; i.e., LDAP Server 26 . In addition, Blanco discloses returning authentication result [access denied/granted in FIG.2] of either successful to access [Grant Access 112 in FIG.3] or sending an unsuccessful to access [Deny Access 106 in FIG.3].

Claim 5

Appellant argues that, the cited portions of Kaufman have not been shown not to specifically disclose or suggest sending of a UserID and the credential string avoids at least one of sending a user's password outside of a portal server and storing the password in a persistent memory.

Examiner would point out that, Kaufman discloses protecting confidentiality of user's password during remote login authentication without transmitting the password over the network [abstract, lines 10-13]; and as clearly seen in FIGS.3-5 of Kaufman's password is not stored in persistent memory because when a user logs into a workstation, the login protocol on the workstation computes two hash totals of the password [FIGS.3-5 and col.4, lines 27-36].

Claim 13

Appellant argues that, the cited portions of Blanco have not been shown not to specifically disclose or suggest validating the confirmation request by assuring that the credential string has been received only once for confirmation at the portal, otherwise, if presented more than once, performing at least one of initiating a security breach procedure and notifying a software application proxy.

Examiner would point out that, as clearly FIGS.2 and 3 Blanco discloses access request is done only once. In other words, Blanco either grants or denies the access request the first request; i.e., re-entering authentication credential is not allowed.

Claims 8, 10 and 14

Appellant argues that, Claims 8, 10 and 14 are dependent claims, depending from distinguishable independent claims.

Examiner would point out that, arguments with respect to the independent claims have been traversed as indicated above; and therefore, arguments with respect to claims 8, 10 and 14 are traversed with the same rationale thereto.

Argument (B):

Appellant argues that the rejection of Claims 6, 7, 15, 19 and 23-25 under 35 U.S.C. 103(a) as being unpatentable over Young (US 7,024,690) in view of Kaufman (US 5,497,421), and further in view of Wenisch (US 7,100,054) is in error, the decision of the Examiner to reject this claim should be reversed, and the application should be remanded to the Examiner.

Examiner respectfully disagrees.

Claim 15

Appellant argues that, Kaufman does not maintain the user password on the portal and avoid exposing the user password to network resources beyond the portal.

Examiner would point out that, Kaufman's password is not maintained on the portal because when a user logs into a workstation, the login protocol computes two hash totals of the password col.4, lines 27-36]. Kaufman also discloses, "In another aspect of the invention, a login protocol enables remote authentication of the user password without transmitting the password over the network" [abstract, lines

10-13]. In addition, Kaufman discloses protecting confidentiality of user's password during remote login authentication without transmitting the password over the network [col.3, line 66 to col.4, line 14].

Appellant argues that, a private RSA key is not a password.

Examiner would point out that, the private RSA key of Kaufman was not equated with a user password in any of the previous rejections.

Appellant further argues that, Wenisch does not maintain the user password on the portal and avoid exposing the user password to network resources beyond the portal.

Examiner would point out that, Wenisch is applied to address other claimed feature of the invention [wherein the credential string validation component checks whether the credential string has been previously received for validation within a predetermined time period] Thus, as explained above Kaufman, not Wenisch, is the reference that is applied to reject the feature 'maintain the user password on the portal and avoid exposing the user password to network resources beyond the portal' [see response to the first argument].

Claims 6, 7, 19 and 23-25

Appellant argues that, Claims 6, 7, 19 and 23-25 are dependent claims, depending from distinguishable independent claims.

Examiner would point out that, arguments with respect to the independent claims have been traversed as indicated above; and therefore, arguments with respect to claims 6, 7, 19 and 23-25 are traversed with the same rationale thereto.

Argument (C):

Appellant argues that the rejection of Claims 16-18 and 21 under 35 U.S.C. 103(a) as being unpatentable over Young (US 7,024,690) in view of Kaufman (US 5,497,421) and Wenisch et al. (US

7,100,054), and further in view of Blanco (US 6,539,482) is in error, the decision of the Examiner to reject this claim should be reversed, and the application should be remanded to the Examiner.

Examiner respectfully disagrees.

Claims 16-18 and 21

Appellant argues that, Claims 16-18 and 21 are dependent claims, depending from distinguishable independent claims.

Examiner would point out that, arguments with respect to the independent claims have been traversed as indicated above; and therefore, arguments with respect to claims 16-18 and 21 are traversed with the same rationale thereto.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/Amare Tabor/

Conferees:

Christopher Brown

/Christopher J Brown/

Primary Examiner, Art Unit 2434

Kambiz Zand

/Kambiz Zand/

Supervisory Patent Examiner, Art Unit 2434